ETSI TECHNICAL REPORT

ETR 295

August 1996

Source: ETSI TC-RES

Reference: DTR/RES-06020

ICS: 33.060

Key words: TETRA, SIM

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); User requirements for Subscriber Identity Module (SIM)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 8

4 General requirements 9

5 Inter-operability 10

6 Support of non-standard applications 10

7 Security 10

8 SIM functions 10

9 Data storage requirements 11
9.1 Data access conditions 11

Annex A: Extract from requirements of TAA1 12

History 13

Blank page

Foreword

This ETSI Technical Report (ETR) has been prepared by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or I-ETS.

Blank page

1 Scope

This ETSI Technical Report (ETR) outlines the technical requirements specification of the Subscriber Identity Module (SIM) for the Trans-European Trunked Radio (TETRA) system. It represents the evolutionary development of the European Telecommunication Standards (ETSs) for TETRA.

This ETR provides the starting point for the system design, and it is the main criteria against which alternative system designs can be judged. It introduces some logical grouping of functions but it should remain implementation independent.

The SIM described in this ETR is a removal IC card. The SIM is an optional device within TETRA Mobile Stations (MSs) and this ETR does not preclude the implementation of MSs without a SIM.

The TETRA SIM may be realized through standards developed by ETSI, ETSI-CEG, ISO or other groups, particularly with reference to the physical specification.

The TETRA SIM should be considered as a data store for the individual TETRA user.

For information only there is an annex to this ETR.

2 References

For the purposes of this ETR, the following reference applies:

[1] prETS 300 392-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETR, the following definitions apply:

access conditions: A set of security attributes associated with a file.

application: An application consists of a set of mechanisms, files, data and protocols (excluding transmission protocols).

authentication: The act of positively verifying that the true identity of an entity (network, user) is the same as the claimed identity.

bearer service: A type of telecommunication service that provides the capability for the transmission of signals between user-network interfaces.

card session: A link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card.

Dedicated File (DF): A file containing access conditions and, optionally, Elementary Files (EFs) or other DFs.

directory: General term for MF and DF.

Elementary File (EF): A file containing access conditions and data and no other files.

encryption: The conversion of plain text to cipher text.

end-to-end: Is within the TETRA boundaries:

- from TETRA terminal to TETRA terminal (LS or MS);
- from TETRA terminal to gateways;
- including Inter-System Interface (ISI).

file: A directory or an organized set of bytes or records in the SIM.

inter-operability: An attribute that describes the ability of a given subscriber terminal to obtain service from a given infrastructure, using the appropriate standard TETRA interface protocols.

key: A sequence of symbols that controls the operations of encipherment and decipherment.

key management: The generation, selection, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

Location Area (LA): An area within a TETRA network that may comprise one, several or all cells. A MS may move freely without re-registering within a LA. A MS has continuity of service within a LA. A LA is geographically static.

Master File (MF): The unique mandatory file containing access conditions and optionally DFs and/or EFs.

migration: The change of LA, each belonging to a different TETRA network.

mobility: The act of a subscriber terminal changing its physical location.

Mobile Station (MS): A physical grouping that contains all of the mobile equipment that is used to obtain TETRA services. By definition, a MS contains at least one Mobile Radio Stack (MRS).

network: A collection of subscriber terminals interconnected through telecommunications devices.

plain text: Information (including data) which is intelligible to all entities.

process: The exact mechanism whereby a given service is performed.

Registered Area (RA): The total area for which a MS is currently registered. The RA is defined by the list of LAs contained in the latest successful registration.

registration: A function which allows a MS to tell the TETRA network that it has changed LA (roaming or migration), TETRA subscriber identity or mode of operation. This function enables the network to keep track of the MS.

roaming: The change of LA within the same TETRA network.

service: One of bearer service, teleservice, or supplementary service that in TETRA provides communications between two or more points in a TETRA system.

supplementary service: A supplementary service modifies or supplements a bearer service or a teleservice. A supplementary service cannot be offered to a customer as a stand alone service. It has to be offered in combination with a bearer service or a teleservice.

teleservice: A type of telecommunications service that provides the complete capability, including terminal equipment functions, for communication between users according to agreed protocols.

3.2 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

ACL	Access Control List
ATR	Answer To Reset
CCK	Common Cipher Key
CHV	Card Holder Verification
DCK	Derived Cipher Key
DF	Dedicated File
EF	Elementary File
ETSI CEG	ETSI Card Expert Group
GTSI	Group TETRA Subscriber Identity

IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ITSI	Individual TETRA Subscriber Identity
LA	Location Area
LME	Layer Management Entity
MCC	Mobile Country Code
MF	Master File
MNC	Mobile Network Code
MRS	Mobile Radio Stack
MS	Mobile Station
RA	Registered Area
SIM	Subscriber Identity Module
TETRA	Trans-European Trunked RAdio
UNBLOCK CHV	Value to unblock CHV

4 General requirements

The SIM is a device to provide secure storage of data, in which data is accessible only through a prescribed interface.

The SIM is a device that should provide authentication of the user to the card and to the mobile, and that will also provide for authentication of the user/mobile-station pair to the network.

The TETRA SIM should consider the following:

- the SIM should be a removable device;
- an operating system should exist in the SIM that provides an Access Control List (ACL), or similar process for verification of data access;
- the SIM module should be in the form of an IC card device in which case the following should be considered:
    - physical dimensions should be as specified by ETSI CEG;
    - electrical interfaces should be as specified by ETSI CEG;
    - the card may be printed or embossed with additional manufacturer data within the limits given by ETSI CEG;
- data storage should be controlled by the Layer Management Entity (LME) of the TETRA protocol stack;
- real time processing should be carried out in the terminal;
- off-line processing (e.g. authentication functions, initialisation functions) may be carried out in the SIM;
- the SIM and its terminal should be treated as co-operative devices and not as stand-alone devices (i.e. a SIM exists only when treated as part of a terminal, a terminal exists only as a complete entity when a SIM exists).

The SIM also has to have the following characteristics:

- all applications on the SIM have to be uniquely identifiable;
- all TETRA SIM applications have to be registered in ETSI;
- the terminal has to verify its ability to use the SIM application on power up;
- the SIM and terminal have to be treated as an indivisible pair during operation.

The SIM should act as host of the TETRA authentication algorithm set specified in ETS 300 392-7 [1]. The implementation of this algorithm is described more fully in document reference ETSI STC RES 06 (95) 086, "Requirements Specification for the TETRA Authentication and Key Management Algorithms set 1 (TAA1)", subclause 9.4. (See annex A).

5 Inter-operability

It should be possible for terminals from any manufacturer to read from a SIM from any other manufacturer.

The terminal equipment has to be able to interrogate the SIM application identity and to enable the equipment operation if the SIM application is supported by the terminal.

All SIM card applications that comply with the TETRA SIM ETS should be registered as TETRA applications by ETSI.

6 Support of non-standard applications

A general purpose IC Card that is used as a SIM may host non-TETRA applications and these should be registered either in ETSI or in ISO.

If non-ETSI applications, or non-TETRA applications, co-exist on the SIM there should be no interference with TETRA data or commands.

7 Security

The storage of secure information on a removable SIM should consider the following rules in addition to those defined by ETSI-CEG and ETSI-TE9:

- dynamic data should be stored on the SIM only for the lifetime of the function using the data (e.g. short term keys (Derived Cipher Key (DCK), Common Cipher Key (CCK));

  NOTE: DCK has a lifetime equal to the time from a successful authentication until one of a new authentication demand, an Individual TETRA Subscriber Identity (ITSI) detach, or power down of the mobile station.

- the terminal and SIM act as a pair and breaking of the relationship between the pair should result in cessation of current operation (i.e. removal of SIM from the terminal should result in the immediate loss of the call and all registration parameters);

- there should be a mechanism of verifying the identity of the card holder by means of CHV;

- there should be a mechanism of verifying the subscriber identity to the network;

- if the secret key "K" is stored on the card it should not be readable via the card interface;

- data access should be protected by means of an Access Control List (ACL).

8 SIM functions

The TETRA SIM applications include the following functional groups:

- authentication and key management as defined in ETS 300 392-7 [1];

- terminal initialization;

- terminal personalization;

- end-to-end encryption key management.

The functions should be initiated by a command set approved by ETSI-CEG as not likely to cause conflict in a multi-application card.

9 Data storage requirements

The TETRA SIM should be considered as a data store for the individual TETRA user. Table 1 identifies that data which is considered static. Static data has a lifetime equal to the lifetime of the card (itself less than or equal to the lifetime of the ITSI). All other data may be considered as dynamic with a lifetime greater than a card session and needs to be maintained on the card when powered down. Dynamic data of this type may be changed during the lifetime of the card.

It should therefore allow the storage of the items indicated in table 1.

Table 1: Static data

ITSI	Individual Tetra Subscriber Identity	48 bits	Static	
	User Name Alias	40 chars		Common name of user associated with the ITSI (may be used for display)
GTSIs	Group TETRA Subscriber Identity	48 bits		This should allow for storage of the GTSIs to which the subscriber is permanently assigned
	Group Name Alias	40 chars each		Common name of group associated with each GTSI (may be used for display)
K	User Secret Key	128 bits	Static	This should not be readily accessible and is used only by the authentication algorithm
SCK	Static Cipher Keys	80 bits by 32 keys		Location in a storage stack should equate to SCKn.
MNC	Mobile Network Code	14 bits	Static	Used by mobility management in roaming and migration. Is part of ITSI
MCC	Mobile Country Code	10 bits	Static	Used by mobility management in roaming and migration. Is part of ITSI
Migration profile	Allowed MCC/MNC values	24 bits each		Pre-determined migration profile
End-to-end key	Key for end-to-end encryption	128 bits each		One key required for each distinct end-to-end encryption unit installed
	SDS Message alias	40 chars each		Text string that should be displayed upon receipt of either STATUS or SDS-1,2,3 message
	Supplementary Service Profile	bitmap 40 bits		To identify which supplementary services may be used by a subscriber
	SCK Alias Stream	TBA		To be aligned with ETS 300 392-7 [1]
Directory	Address-Alias	48 bits + alias		To provide displayable address book for ITSI and/or GTSI

9.1 Data access conditions

The relationships between data elements should be considered. Deletion and/or update of an element should not alter its relationship with any other element.

It may be appropriate to define the data model of the TETRA SIM using Structured Query Language (SQL) and/or entity relationship diagrams. Where the data is protected by an interface protocol the interface may be defined using Specification Description Language (SDL).

Annex A: Extract from requirements of TAA1

NOTE: This extract retains the clause numbering of the source document

"9.4 Implementation and operational considerations

The algorithm should be designed for software implementations and specifically for implementations in the processors of IC cards.

The set of the algorithms should be implementable on a 6805 family of microprocessors, in particular the Motorola SC21 series and Philips 83C852 series, running at 4 MHz. Given this environment it should be possible to realize an efficient state of the art implementation such that:

- for each of the algorithms TA11, TA12, TA21, TA22, TA41 the time for one operation is less than 80 ms;
- for each of the algorithms TA31, TA32, TA51, TA52 the time for one operation is less than 150 ms;
- for each of the algorithms TB1, TB2, TB3, TB4 the time for one operation is less than 20 ms;
- the complete set of algorithms can be implemented using less than 2 000 bytes ROM and 64 bytes RAM."

History

Document history	
August 1996	First Edition

ISBN 2-7437-0705-4
Dépôt légal : Août 1996